UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/919,958	08/02/2001	Bruno Couillard	47-16 US	4261

25319 7590 02/24/2005

FREEDMAN & ASSOCIATES
117 CENTREPOINTE DRIVE
SUITE 350
NEPEAN, ONTARIO, K2G 5X3
CANADA

EXAMINER	
PYZOCHA, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2137	

DATE MAILED: 02/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/919,958	COUILLARD, BRUNO	
	Examiner	Art Unit	
	Michael Pyzocha	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *02 August 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *02 August 2001* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *01062004*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 are pending.

Claim Rejections - 35 USC § 112

2. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 7-10 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

4. The term "sufficiently large" in claim 7 is a relative term which renders the claim indefinite. The term "sufficiently large" is not defined by the claim, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. It will be assumed the unique code in a timestamp of 512 bits will be sufficiently large.

Claim Rejections - 35 USC § 102

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless -
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claim 19 is rejected under 35 U.S.C. 102(b) as being anticipated by Fischer (US 5001752).

As per claim 19, Fischer discloses receiving securely time stamped digital data, wherein the securely time stamped digital data have a unique code embedded therein, and wherein the unique code has been generated by a processor after the processor has been placed in a mode of operation in which a secure encryption key is only used for time stamping operations; decrypting the timestamp using a key corresponding to the secure encryption key for providing time data in dependence thereupon; retrieving the unique code from the securely time stamped digital data; and, comparing the unique code with reference data in order to produce a comparison result, and if the comparison result is indicative of a match indicating authenticity of the time data (see column 8 line 51 through column 9 line 22).

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-18, and 20-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Fischer (US 5001752), further in view of Goodman (US 6466048), and further in view of Menezes et al (Handbook of Applied Cryptography).

As per claims 1 and 20, Fischer discloses a processor for per forming time stamping operations with a secure encryption key (see Fig 1 and column 2 lines 12-23).

Fischer fails to disclose the system having two separate modes.

However, Goodman teaches two different modes (see column 8 lines 53-67 and column 7 lines 29-55).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Goodman's different modes in the time stamping system of Fischer.

Motivation to do so would have been to allow the checking of the processes being performed by the processor (see Goodman column 8 lines 53-67).

The modified Fischer and Goodman system fails to disclose precluding the first mode to use the secure key after being used in the second mode.

However, Menezes et al teaches the use of session keys (see page 494) which are used for only one transmission.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Menezes et al's idea of session keys to prevent to key from being used again after time stamping operations have been performed.

Motivation to do so would have been to create independence across communications sessions and applications (see Menezes et al page 494).

As per claim 2, the modified Fischer, Goodman, and Menezes et al system discloses receiving a request to perform a time stamping operation and placing the processor in the second mode of operation once the request is received (see Goodman column 7 lines 29-55).

As per claim 3, the modified Fischer, Goodman, and Menezes et al system discloses generating a unique code for being embedded within time stamped digital data, wherein the secure

encryption key and the processor are within a secure module and wherein the unique code is indeterminable outside the secure module prior to receipt of the request (see Fischer column 4 line 61 through column 5 line 17).

As per claims 4, 11 and 15, the modified Fischer, Goodman, and Menezes et al system discloses the step of generating a unique code for being embedded within time stamped digital data, the unique code being indeterminable before receipt of the request (see Fischer column 4 line 61 through column 5 line 17).

As per claim 5, the modified Fischer, Goodman, and Menezes et al system discloses the unique code is inserted within each time stamped digital data (see Fischer column 4 line 61 through column 5 line 17).

As per claim 6, the modified Fischer, Goodman, and Menezes et al system discloses each time stamped digital data comprises a timestamp, and wherein the unique code is encoded within the timestamp (see Fischer column 6 lines 25-46).

As per claim 7, the modified Fischer, Goodman, and Menezes et al system discloses the unique code is sufficiently large to dissuade brute force attacks (see Fischer column 5 lines 1-17 and column 8 lines 25-46).

As per claim 8, the modified Fischer, Goodman, and Menezes et al system discloses the unique code is generated based on a random number (see Fischer column 5 lines 1-17).

As per claim 9, the modified Fischer, Goodman, and Menezes et al system discloses the unique code is generated based on a random number (see Fischer column 5 lines 1-17).

As per claim 10, the modified Fischer, Goodman, and Menezes et al system discloses the unique code is generated based on a real time value indicative of a time instance of a first request has been received (see Fischer column 6 lines 25-46).

As per claims 12-13 and 16-18, the modified Fischer, Goodman, and Menezes et al system discloses receiving from a real time clock data indicative of a real time the first request for a time stamping operation has been received; generating a first timestamp based on the data indicative of real time using the secure encryption key; embedding the first timestamp within the first digital data and inserting the unique code within the first digital data; and, encoding the first digital data with inserted data therein to form time stamped digital data (see Goodman as above for the request and see Fischer column 6 lines 9-46 which also discloses the data being hashed as in claim 17).

As per claim 14, the modified Fischer, Goodman, and Menezes et al system discloses this limitation as in claims above being repeated for a second request.

As per claim 21, the modified Fischer, Goodman, and Menezes et al system discloses a real time clock for providing data indicative of a real time (see Fischer Fig 1).

As per claim 22 the modified Fischer, Goodman, and Menezes et al system discloses the processor generates a secure encryption key (see Fischer column 8 lines 12-50).

As per claim 23, the modified Fischer, Goodman, and Menezes et al system discloses the step of generating a unique code for being embedded within time stamped digital data, the unique code being indeterminable before receipt of the request (see Fischer column 4 line 61 through column 5 line 17).

As per claim 24, the modified Fischer, Goodman, and Menezes et al system discloses generating a unique code for being embedded within time stamped digital data, wherein the secure encryption key and the processor are within a secure module and wherein the unique code is indeterminable outside the secure module prior to receipt of the request (see Fischer column 4 line 61 through column 5 line 17).

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Berson et al (US 5949879) discloses a method of time stamping with testing, Schneier et al (US 5956404) disclose a method of digitally signing a document with a time stamp, and Davis (US 5966446) discloses a method of time stamping.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

ANDREW CALDWELL
SUPERVISORY PATENT EXAMINER